

# Admin API Documentation

## Overview / نظرة عامة

This document describes the admin API endpoints for comprehensive user management in the Magnet project.

Magnet للمدير لإدارة شاملة للمستخدمين في مشروع API هذا المستند يصف نقاط نهاية

## Authentication & Authorization / المصادقة والتفويض

All admin endpoints require:

- **Authentication:** Valid JWT token in **Authorization: Bearer <token>** header
- **Authorization:** User must have **admin** role

جميع نقاط نهاية المدير تتطلب:

- **Authorization: Bearer <token>** صالح في رأس **JWT المصادقة**: رمز
- **admin التفويض**: يجب أن يكون للمستخدم دور

## Base URL / الرابط الأساسي

```
/api/admin
```

## User Management Endpoints / نقاط نهاية إدارة المستخدمين

### 1. Create User / إنشاء مستخدم

**POST** `/api/admin/users`

Creates any type of user (customer, business, magnet\_employee, admin).

(مدير، magnet، إنشاء أي نوع من المستخدمين (عميل، عمل، موظف).

### Request Body / جسم الطلب

```
{
  "firstname": "John",
  "lastname": "Doe",
  "email": "john.doe@example.com",
  "phone": "+966501234567",
  "password": "SecurePassword123",
  "role": "business",
}
```

```
"country": "Saudi Arabia",
"language": "en",
"crNumber": "CR123456",
"vatNumber": "VAT123456",
"companyName": "Example Company",
"companyType": "LLC",
"city": "Riyadh",
"district": "Al Olaya",
"streetName": "King Fahd Road"
}
```

Required Fields by Role / الحقول المطلوبة حسب الدور

Role / الدور	Required Fields / الحقول المطلوبة
customer	firstname, lastname, email, password, country
business	firstname, lastname, email, password, country, crNumber, vatNumber, companyName, companyType, city, district, streetName
magnet_employee	firstname, lastname, email, password, country
admin	firstname, lastname, email, password, country

Response / الاستجابة

```
{
  "status": "success",
  "data": {
    "user": {
      "id": "60f7b3b3b3b3b3b3b3b3b3b3",
      "firstname": "John",
      "lastname": "Doe",
      "email": "john.doe@example.com",
      "phone": "+966501234567",
      "role": "business",
      "country": "Saudi Arabia",
      "language": "en",
      "isEmailVerified": true,
      "isPhoneVerified": true,
      "isDisallowed": false,
      "businessInfo": {
        "crNumber": "CR123456",
        "vatNumber": "VAT123456",
        "companyName": "Example Company",
        "companyType": "LLC",
        "city": "Riyadh",
        "district": "Al Olaya",
        "streetName": "King Fahd Road",
        "isApproved": true,
        "approvalStatus": "approved"
      }
    }
  }
}
```

```
    },
    "createdAt": "2024-01-15T10:30:00.000Z",
    "updatedAt": "2024-01-15T10:30:00.000Z"
  }
},
"message": {
  "en": "User created successfully",
  "ar": "تم إنشاء المستخدم بنجاح"
}
}
```

## 2. Get All Users / الحصول على جميع المستخدمين

**GET** /api/admin/users

Retrieves all users with pagination, filtering, and search capabilities.

استرجاع جميع المستخدمين مع الترتيم والتصفيه وإمكانيات البحث

### Query Parameters / معاملات الاستعلام

Parameter / المعامل	Type / النوع	Description / الوصف
page	number	Page number (default: 1)
limit	number	Items per page (default: 10)
role	string	Filter by role (customer, business, magnet_employee, admin)
status	string	Filter by status (active, disallowed)
search	string	Search in name, email, phone, company name
sortBy	string	Sort field (default: createdAt)
sortOrder	string	Sort order (asc, desc)

### Example Request / مثال على الطلب

```
GET /api/admin/users?
page=1&limit=10&role=business&status=active&search=company&sortBy=createdAt&sortOrder=desc
```

### Response / الاستجابة

```
{
  "status": "success",
  "data": {
    "users": [
```

```
{
  "id": "60f7b3b3b3b3b3b3b3b3b3b3",
  "firstname": "John",
  "lastname": "Doe",
  "email": "john.doe@example.com",
  "phone": "+966501234567",
  "role": "business",
  "country": "Saudi Arabia",
  "language": "en",
  "isEmailVerified": true,
  "isPhoneVerified": true,
  "isDisallowed": false,
  "businessInfo": {
    "companyName": "Example Company",
    "approvalStatus": "approved"
  },
  "createdAt": "2024-01-15T10:30:00.000Z"
}
],
"pagination": {
  "currentPage": 1,
  "totalPages": 5,
  "totalItems": 50,
  "itemsPerPage": 10
}
}
```

---

### 3. Get User Statistics / إحصائيات المستخدمين

**GET** /api/admin/users/stats

Retrieves comprehensive user statistics.

استرجاع إحصائيات شاملة للمستخدمين.

#### Response / الاستجابة

```
{
  "status": "success",
  "data": {
    "stats": {
      "total": 150,
      "byRole": {
        "customers": 80,
        "businesses": 45,
        "employees": 15,
        "admins": 10
      }
    },
    "byStatus": {
```

```

    "active": 140,
    "disallowed": 10
  },
  "businessApproval": {
    "pending": 5,
    "approved": 35,
    "rejected": 5
  }
}
}
}

```

#### 4. Get User by ID / الحصول على مستخدم بالمعرف

**GET** /api/admin/users/:id

Retrieves a specific user by their ID.

استرجاع مستخدم محدد بواسطة المعرف.

#### Response / الاستجابة

```

{
  "status": "success",
  "data": {
    "user": {
      "id": "60f7b3b3b3b3b3b3b3b3b3b3",
      "firstname": "John",
      "lastname": "Doe",
      "email": "john.doe@example.com",
      "phone": "+966501234567",
      "role": "business",
      "country": "Saudi Arabia",
      "language": "en",
      "isEmailVerified": true,
      "isPhoneVerified": true,
      "isDisallowed": false,
      "businessInfo": {
        "crNumber": "CR123456",
        "vatNumber": "VAT123456",
        "companyName": "Example Company",
        "companyType": "LLC",
        "city": "Riyadh",
        "district": "Al Olaya",
        "streetName": "King Fahd Road",
        "isApproved": true,
        "approvalStatus": "approved"
      },
      "createdAt": "2024-01-15T10:30:00.000Z",
      "updatedAt": "2024-01-15T10:30:00.000Z"
    }
  }
}

```

```
}  
}  
}
```

## 5. Update User / تحديث مستخدم

**PUT** /api/admin/users/:id

Updates a user's information.

تحديث معلومات المستخدم.

### Request Body / جسم الطلب

```
{  
  "firstname": "John Updated",  
  "lastname": "Doe Updated",  
  "email": "john.updated@example.com",  
  "phone": "+966501234568",  
  "password": "NewSecurePassword123",  
  "role": "business",  
  "country": "Saudi Arabia",  
  "language": "ar",  
  "isEmailVerified": true,  
  "isPhoneVerified": true,  
  "isDisallowed": false,  
  "crNumber": "CR123456",  
  "vatNumber": "VAT123456",  
  "companyName": "Updated Company",  
  "companyType": "LLC",  
  "businessCity": "Jeddah",  
  "businessDistrict": "Al Hamra",  
  "businessStreetName": "King Abdulaziz Road"  
}
```

### Response / الاستجابة

```
{  
  "status": "success",  
  "data": {  
    "user": {  
      "id": "60f7b3b3b3b3b3b3b3b3b3b3b3b3b3b3",  
      "firstname": "John Updated",  
      "lastname": "Doe Updated",  
      "email": "john.updated@example.com",  
      "phone": "+966501234568",  
      "role": "business",  
      "country": "Saudi Arabia",  

```

```
{
  "language": "ar",
  "isEmailVerified": true,
  "isPhoneVerified": true,
  "isDisallowed": false,
  "businessInfo": {
    "crNumber": "CR123456",
    "vatNumber": "VAT123456",
    "companyName": "Updated Company",
    "companyType": "LLC",
    "city": "Jeddah",
    "district": "Al Hamra",
    "streetName": "King Abdulaziz Road",
    "isApproved": true,
    "approvalStatus": "approved"
  },
  "createdAt": "2024-01-15T10:30:00.000Z",
  "updatedAt": "2024-01-15T11:30:00.000Z"
},
{
  "message": {
    "en": "User updated successfully",
    "ar": "تم تحديث المستخدم بنجاح"
  }
}
```

---

## 6. Delete User / حذف مستخدم

**DELETE** /api/admin/users/:id

Deletes a user permanently.

حذف المستخدم نهائياً.

**Response / الاستجابة**

```
{
  "status": "success",
  "message": {
    "en": "User deleted successfully",
    "ar": "تم حذف المستخدم بنجاح"
  }
}
```

---

## 7. Disallow User / منع مستخدم

**PUT** /api/admin/users/:id/disallow

Disallows a user from logging in or performing actions.

منع المستخدم من تسجيل الدخول أو تنفيذ الإجراءات.

### Request Body / جسم الطلب

```
{
  "reason": "Violation of terms of service"
}
```

### Response / الاستجابة

```
{
  "status": "success",
  "data": {
    "user": {
      "id": "60f7b3b3b3b3b3b3b3b3b3b3",
      "firstname": "John",
      "lastname": "Doe",
      "email": "john.doe@example.com",
      "role": "business",
      "isDisallowed": true,
      "disallowReason": "Violation of terms of service",
      "disallowedBy": "60f7b3b3b3b3b3b3b3b3b3b4",
      "disallowedAt": "2024-01-15T12:00:00.000Z",
      "updatedAt": "2024-01-15T12:00:00.000Z"
    }
  },
  "message": {
    "en": "User disallowed successfully",
    "ar": "تم منع المستخدم بنجاح"
  }
}
```

---

## 8. Allow User / السماح للمستخدم

**PUT** /api/admin/users/:id/allow

Allows a previously disallowed user to login and perform actions.

السماح لمستخدم محظور سابقاً بتسجيل الدخول وتنفيذ الإجراءات.

### Response / الاستجابة

```
{
  "status": "success",
  "data": {
    "user": {
```



```
    "id": "60f7b3b3b3b3b3b3b3b3b3b3b3b3b3",
    "firstname": "John",
    "lastname": "Doe",
    "email": "john.doe@example.com",
    "role": "business",
    "isDisallowed": false,
    "allowedBy": "60f7b3b3b3b3b3b3b3b3b3b3b3b3b4",
    "allowedAt": "2024-01-15T13:00:00.000Z",
    "updatedAt": "2024-01-15T13:00:00.000Z"
  }
},
"message": {
  "en": "User allowed successfully",
  "ar": "تم السماح للمستخدم بنجاح"
}
}
```

## Error Responses / استجابات الأخطاء

Common Error Codes / رموز الأخطاء الشائعة

Status Code / رمز الحالة	Description / الوصف
400	Bad Request - Invalid input data
401	Unauthorized - Missing or invalid token
403	Forbidden - Insufficient permissions
404	Not Found - User not found
500	Internal Server Error

Example Error Response / مثال على استجابة الخطأ

```
{
  "status": "error",
  "message": {
    "en": "User not found",
    "ar": "المستخدم غير موجود"
  }
}
```

## Security Considerations / اعتبارات الأمان

Admin Protection / حماية المدير

- Admins cannot delete themselves

- Admins cannot disallow themselves
- All admin actions are logged
- Strong password requirements enforced

## User Disallowance / منع المستخدمين

- Disallowed users cannot login
- Disallowed business users cannot add products
- Disallowed users cannot perform any actions
- Disallowance reason is tracked

---

## Usage Examples / أمثلة الاستخدام

### Create a Business User / إنشاء مستخدم عمل

```
curl -X POST /api/admin/users \
-H "Authorization: Bearer <admin_token>" \
-H "Content-Type: application/json" \
-d '{
  "firstname": "Ahmed",
  "lastname": "Al-Sayed",
  "email": "ahmed@company.com",
  "phone": "+966501234567",
  "password": "SecurePass123",
  "role": "business",
  "country": "Saudi Arabia",
  "crNumber": "CR789012",
  "vatNumber": "VAT789012",
  "companyName": "Al-Sayed Trading Co.",
  "companyType": "LLC",
  "city": "Riyadh",
  "district": "Al Olaya",
  "streetName": "King Fahd Road"
}'
```

### Get Users with Filters / الحصول على المستخدمين مع المرشحات

```
curl -X GET "/api/admin/users?
role=business&status=active&search=company&page=1&limit=10" \
-H "Authorization: Bearer <admin_token>"
```

### Disallow a User / منع مستخدم

```
curl -X PUT /api/admin/users/60f7b3b3b3b3b3b3b3b3b3b3/disallow \
-H "Authorization: Bearer <admin_token>" \
-H "Content-Type: application/json" \
```

```
-d '{  
  "reason": "Multiple terms of service violations"  
}'
```

---

## Notes / ملاحظات

1. **Business Users:** When creating business users, they are automatically approved
2. **Password Security:** All passwords are hashed using bcrypt
3. **Email Verification:** Admin-created users are automatically email verified
4. **Phone Verification:** Admin-created users with phone numbers are automatically phone verified
5. **Disallowance:** Disallowed users cannot perform any actions in the system
6. **Audit Trail:** All admin actions are tracked with timestamps and admin IDs
7. **مستخدمي الأعمال:** عند إنشاء مستخدمي الأعمال، يتم الموافقة عليهم تلقائياً
8. **bcrypt أمان كلمة المرور:** جميع كلمات المرور مشفرة باستخدام bcrypt
9. **التحقق من البريد الإلكتروني:** المستخدمون المنشأون من قبل المدير يتم التحقق من بريدهم الإلكتروني تلقائياً
10. **التحقق من الهاتف:** المستخدمون المنشأون من قبل المدير مع أرقام الهاتف يتم التحقق من هواتفهم تلقائياً
11. **المنع:** المستخدمون المحظورون لا يمكنهم تنفيذ أي إجراءات في النظام
12. **مسار التدقيق:** جميع إجراءات المدير يتم تتبعها مع الطوابع الزمنية ومعرفات المدير